IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Lifestream Technologies, Inc.**

Serial No.: **filed herewith**

Inventor: **MAUS, et. al.**

Filed: **November 8, 1999**

For: **HEALTH MONITORING AND DIAGNOSTIC DEVICE AND NETWORK-BASED HEALTH ASSESSMENT AND MEDICAL RECORDS MAINTENANCE SYSTEM**

Group Art No. 1743

Examiner: SIEFKE, Samuel P.

CLAIMS LISTING AFTER AMENDMENT DATED AUGUST 26, 2003

1-33 Cancelled.

34. (Original) A secure medical records maintenance system, comprising:

a plurality of removable memory storage devices, each operable for storing medical data for an associated patient, a patient-specified personal identification number, and a medical records identification number secured by the patient-specified personal identification number;

a first remote server operable for storing patient identification information indexed patient identification numbers;

a second remote server operable for storing patient medical data indexed by the medical records identification numbers; and

the medical data maintained in the second remote server cannot be correlated to the associated patient identification information maintained in the first remote server based on the information contained in the first and second remote servers.

35. (Original) The secure medical records maintenance system of claim 34, wherein each removable memory storage device also stores a patient identification number corresponding to the medical records identification number stored on the removable memory storage.

36. (Original) The secure medical records maintenance system of claim 34, further comprising a correlation table uniquely associating each medical records identification number with a particular one of the patient identification numbers.

37. (Original) The secure medical records maintenance system of claim 36, wherein:

the correlation table resides on a practitioner computer associated with a licensed medical practitioner having an assigned professional registration number; and

the first and second remote servers can be accessed by the practitioner computer through encrypted communications secured by an application procedure comprising validation of the practitioner's registration number.

38. (Original) The secure medical records maintenance system of claim 37, wherein the application procedure further comprises receipt and validation of a client-supplied personal identification number.

39. (Original) The secure medical records maintenance system of claim 38, wherein the application procedure comprises issuance of a client certificate insuring that access to the first and second remote servers occurs from the practitioner's computer.

40. (Original) The secure medical records maintenance system of claim 34, wherein access is granted to the first remote server, but not to the second server, for the purpose of generating a mailing list of patients without divulging any medical data associated with the patients.

41. (Original) The secure medical records maintenance system of claim 34, wherein access is granted to the second remote server, but not to the first server, for the purpose of conducting investigative analyses involving patient medical data without divulging any patient identification information associated with the patients.

42. (Original) The secure medical records maintenance system of claim 34, wherein the medical data stored on each removable memory storage device is automatically erased from the memory storage device after the data is entered into the second remote server.

43. (Original) The secure medical records maintenance system of claim 34, wherein the removable memory storage device is receivable within a hand-held health monitoring device operable for storing the medical data on the removable memory storage device.

44. (Original) The secure medical records maintenance system of claim 34, wherein the removable memory storage device is receivable within a computer operable for transmitting the medical data to the second remote server over the Internet.

45-49 Cancelled.